

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

- 1 1. (Currently amended) A method ~~for to facilitate secure~~
2 ~~messaging~~enabling a database system to prove that an origin system sent a
3 message, comprising:
4 ~~creating a message at an origin;~~
5 ~~computing a digest of the message;~~
6 ~~signing the digest using an origin private encryption key;~~
7 ~~sending the message and the digest to a queue located in a third party~~
8 ~~device for delivery to a recipient;~~
9 receiving the message and ~~the a signed first digest at the queue of the~~
10 message at a database system from the origin system, wherein the signed first
11 digest was created by signing a digest of the message using an origin private
12 encryption key;
13 using an origin public encryption key that is associated with the origin
14 private encryption key to verifying that the signed first digest was signed at by the
15 origin system, thereby proving that the origin system created and sent the
16 message by using an origin public encryption key, whereby the origin cannot deny
17 creating the message; and
18 persistently storing the signed first digest with the message, thereby
19 enabling the database system to present the signed first digest as proof that the
20 origin system sent the message.
21 ~~if the digest is verified as being signed at the origin,~~

22 placing the message and digest on the queue and
23 persistently storing a record of this transaction, and
24 notifying the recipient that the message is available;
25 generating a request at the recipient to receive the message from the queue
26 located in the third party device;
27 creating a signature for the request using a recipient private encryption
28 key;
29 sending the request and the signature to the queue;
30 validating the request at the queue using the signature and a recipient
31 public encryption key; and
32 if the request is valid,
33 dequeuing the message from the queue;
34 sending the digest to the recipient;
35 signing the digest at the recipient using the recipient private
36 encryption key creating a signed digest;
37 returning the signed digest to the queue;
38 validating the signed digest at the queue using the recipient
39 public encryption key, whereby the recipient cannot deny
40 requesting to receive the message, and
41 if the signed digest is valid, persistently storing a record of
42 this transaction and sending the message to the recipient.

1 2. (Canceled).

1 3. (Currently amended) The method of claim 22-~~claim 4~~, further
2 comprising passing the message and the digest through a plurality of queues
3 between the origin and the recipient, whereby the recipient and the origin are
4 subscribers of different queues.

1 4. (Original) The method of claim 3, further comprising passing the
2 message and the digest through a plurality of databases, wherein each database in
3 the plurality of databases includes at least one queue of the plurality of queues.

1 5. (Previously presented) The method of claim 1, wherein the origin public
2 encryption key and the origin private encryption key are a key pair of a public key
3 encryption system.

1 6. (Currently amended) The method of claim 22-claim 1, wherein the
2 recipient public encryption key and the recipient private encryption key are a key
3 pair of a public key encryption system.

1 7. (Previously presented) The method of claim 1, wherein computing the
2 digest includes using one of message digest 2 (MD2), message digest 4 (MD4),
3 message digest 5 (MD5), secure hash algorithm (SHA), and secure hash algorithm
4 1 (SHA1).

1 8. (Currently amended) A computer-readable storage medium storing
2 instructions that when executed by a computer cause the computer to perform a
3 method to facilitate secure messaging for enabling a database system to prove that
4 an origin system sent a message, the method comprising:
5 creating a message at an origin;
6 computing a digest of the message;
7 signing the digest using an origin private encryption key;
8 sending the message and the digest to a queue located in a third party
9 device for delivery to a recipient;
10 receiving the message and the a signed first digest at the queue of the
11 message at a database system from the origin system, wherein the signed first

12 digest was created by signing a digest of the message using an origin private
13 encryption key;
14 using an origin public encryption key that is associated with the origin
15 private encryption key to verifying that the signed first digest was signed at by the
16 origin system, thereby proving that the origin system created and sent the
17 message by using an origin public encryption key, whereby the origin cannot deny
18 creating the message; and
19 persistently storing the signed first digest with the message, thereby
20 enabling the database system to present the signed first digest as proof that the
21 origin system sent the message.
22 if the digest is verified as being signed at the origin,
23 placing the message and digest on the queue and
24 persistently storing a record of this transaction, and
25 notifying the recipient that the message is available;
26 generating a request at the recipient to receive the message
27 from the queue located in the third party device;
28 creating a signature for the request using a recipient private
29 encryption key;
30 sending the request and the signature to the queue;
31 validating the request at the queue using the signature and a
32 recipient public encryption key; and
33 if the request is valid,
34 dequeueing the message from the queue,
35 sending the digest to the recipient,
36 signing the digest at the recipient using the recipient private
37 encryption key creating a signed digest,
38 returning the signed digest to the queue,

39 | validating the signed digest at the queue using the recipient
40 | public encryption key, whereby the recipient cannot deny
41 | requesting to receive the message, and
42 | if the signed digest is valid, persistently storing a record of this transaction
43 | and sending the message to the recipient.

1 9. (Canceled).

1 | 10. (Currently amended) The computer-readable storage medium of claim
2 | 23-claim 8, the method further comprising passing the message and the digest
3 | through a plurality of queues between the origin and the recipient, whereby the
4 | recipient and the origin are subscribers of different queues.

1 11. (Original) The computer-readable storage medium of claim 10, the
2 | method further comprising passing the message and the digest through a plurality
3 | of databases, wherein each database in the plurality of databases includes at least
4 | one queue of the plurality of queues.

1 12. (Previously presented) The computer-readable storage medium of
2 | claim 8, wherein the origin public encryption key and the origin private encryption
3 | key are a key pair of a public key encryption system.

1 | 13. (Currently amended) The computer-readable storage medium of claim
2 | 23-claim 8, wherein the recipient public encryption key and the recipient private
3 | encryption key are a key pair of a public key encryption system.

1 14. (Previously presented) The computer-readable storage medium of
2 | claim 8, wherein computing the digest includes using one of message digest 2

3 (MD2), message digest 4 (MD4), message digest 5 (MD5), secure hash algorithm
4 (SHA), and secure hash algorithm 1 (SHA1).

1 15. (Currently amended) An apparatus ~~for~~ to facilitate secure messaging
2 enabling a database system to prove that an origin system sent a message,
3 comprising:
4 a ~~first creating mechanism that is configured to create a message at an~~
5 ~~origin;~~
6 a ~~computing mechanism that is configured to compute a digest of the~~
7 ~~message;~~
8 a ~~first signing mechanism that is configured to sign the digest using an~~
9 ~~origin private encryption key;~~
10 a ~~first sending mechanism that is configured to send the message and the~~
11 ~~digest to a queue located in a third party device for delivery to a recipient;~~
12 a first receiving mechanism that is configured to receive the message and
13 the a signed first digest at the queue of the message at a database system from the
14 origin system, wherein the signed first digest was created by signing a digest of
15 the message using an origin private encryption key;
16 a first verifying mechanism that is configured to use an origin public
17 encryption key that is associated with the origin private encryption key to verify
18 that the signed first digest was signed at by the origin system, thereby proving that
19 the origin system created and sent the message by using an origin public
20 encryption key, whereby the origin cannot deny creating the message; and
21 a first storingplacing mechanism that is configured to place persistently
22 store the signed first digest with the message, thereby enabling the database
23 system to present the signed first digest as proof that the origin system sent the
24 message. the message and digest on the queue and persistently store a record of

25 ~~this transaction; a notifying mechanism that is configured to notify the recipient~~
26 ~~that the message is available;~~
27 ~~a generating mechanism that is configured to generate a request at the~~
28 ~~recipient to receive the message from the queue located in the third party device;~~
29 ~~a second creating mechanism that is configured to create a signature for~~
30 ~~the request using a recipient private encryption key;~~
31 ~~a second sending mechanism that is configured to send the request and the~~
32 ~~signature to the queue;~~
33 ~~a first validating mechanism that is configured to validate the request at~~
34 ~~the queue using the signature and a recipient public encryption key;~~
35 ~~a dequeuing mechanism that is configured to dequeue the message from~~
36 ~~the queue;~~
37 ~~a third sending mechanism that is configured to send the digest to the~~
38 ~~recipient;~~
39 ~~a second signing mechanism that is configured to sign the digest at the~~
40 ~~recipient using the recipient private encryption key creating a signed digest;~~
41 ~~a returning mechanism that is configured to return the signed digest to the~~
42 ~~queue;~~
43 ~~a second validating mechanism that is configured to validate the signed~~
44 ~~digest at the queue using the recipient public encryption key and persistently store~~
45 ~~a record of this transaction, whereby the recipient cannot deny requesting to~~
46 ~~receive the message; and~~
47 ~~wherein the third sending mechanism is further configured to send the~~
48 ~~message to the recipient.~~

1 16. (Canceled).

1 | 17. (Currently amended) The apparatus of claim 24 ~~claim 15~~, further
2 comprising a passing mechanism that is configured to pass the message and the
3 digest through a plurality of queues between the origin and the recipient, whereby
4 the recipient and the origin are subscribers of different queues.

1 18. (Original) The apparatus of claim 17, wherein the passing mechanism
2 is further configured to pass the message and the digest through a plurality of
3 databases, wherein each database in the plurality of databases includes at least one
4 queue of the plurality of queues.

1 19. (Previously presented) The apparatus of claim 15, wherein the origin
2 public encryption key and the origin private encryption key are a key pair of a
3 public key encryption system.

1 | 20. (Currently amended) The apparatus of claim 24 ~~claim 15~~, wherein the
2 recipient public encryption key and the recipient private encryption key are a key
3 pair of a public key encryption system.

1 21. (Previously presented) The apparatus of claim 15, wherein computing
2 the digest includes using one of message digest 2 (MD2), message digest 4
3 (MD4), message digest 5 (MD5), secure hash algorithm (SHA), and secure hash
4 algorithm 1 (SHA1).

1 22. (New) The method of claim 1, further comprising:
2 receiving a signed receive-request from a recipient system for receiving
3 the message, wherein the receive-request is signed using a recipient private
4 encryption key;

5 validating the signed receive-request using a recipient public encryption
6 key that is associated with the recipient private encryption key;
7 sending a second digest of the message to the recipient system;
8 receiving a signed second digest from the recipient system, wherein the
9 signed second digest was created by signing the second digest using the recipient
10 private encryption key;
11 validating the signed second digest using the recipient public encryption
12 key, thereby proving that the recipient system requested to receive the message;
13 and
14 persistently storing the signed second digest, thereby enabling the database
15 system to present the signed second digest as proof that the recipient system
16 requested to receive the message.

1 23. (New) The computer-readable storage medium of claim 8, the method
2 further comprising:
3 receiving a signed receive-request from a recipient system for receiving
4 the message, wherein the receive-request is signed using a recipient private
5 encryption key;
6 validating the signed receive-request using a recipient public encryption
7 key that is associated with the recipient private encryption key;
8 sending a second digest of the message to the recipient system;
9 receiving a signed second digest from the recipient system, wherein the
10 signed second digest was created by signing the second digest using the recipient
11 private encryption key;
12 validating the signed second digest using the recipient public encryption
13 key, thereby proving that the recipient system requested to receive the message;
14 and

15 persistently storing the signed second digest, thereby enabling the database
16 system to present the signed second digest as proof that the recipient system
17 requested to receive the message.

1 24. (New) The apparatus of claim 15, further comprising:
2 a second receiving mechanism configured to receive a signed
3 receive-request from a recipient system for receiving the message, wherein the
4 receive-request is signed using a recipient private encryption key;
5 a second validating mechanism configured to validate the signed
6 receive-request using a recipient public encryption key that is associated with the
7 recipient private encryption key;
8 a second sending mechanism configured to send a second digest of the
9 message to the recipient system;
10 a third receiving mechanism configured to receive a signed second digest
11 from the recipient system, wherein the signed second digest was created by
12 signing the second digest using the recipient private encryption key;
13 a third validating mechanism configured to validate the signed second
14 digest using the recipient public encryption key, thereby proving that the recipient
15 system requested to receive the message; and
16 a second storing mechanism configured to persistently store the signed
17 second digest, thereby enabling the database system to present the signed second
18 digest as proof that the recipient system requested to receive the message.